

FILEDUNITED STATES DISTRICT COURT
ALBUQUERQUE, NEW MEXICO

UNITED STATES DISTRICT COURT

DEC 04 2019

for the
District of New MexicoMITCHELL R. ELFERS
CLERKIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Case No.

INFORMATION PRODUCED BY icecreammonmars.com
IN RESPONSE TO 19-MR-1344 AND CURRENTLY IN
THE POSSESSION OF THE FBI

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, attached hereto and incorporated herein.

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, attached hereto and incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 875

Interstate Communications

Offense Description

The application is based on these facts:

See Affidavit, attached hereto and incorporated herein.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Jacob vanBrandwijk, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 12-4-19

City and state: Albuquerque, New Mexico



Judge's signature

Kirtan Khalsa, United States Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF
INFORMATION PRODUCED BY
icecreamonmars.com IN RESPONSE TO 19-
MR-1344 AND CURRENTLY IN THE
POSSESSION OF THE FBI

Case No.

Filed Under Seal

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR AN SEARCH WARRANT

I, Jacob vanBrandwijk, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of criminal Procedure for a warrant to search information produced by icecreamonmars.com in response to 19-MR-1344, hereafter THE PRODUCED INFORMATION, that is currently in the possession of the Federal Bureau of Investigation and is located at 4200 Luecking Park Avenue, Albuquerque, New Mexico, 87107.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since March, 2017. While employed by the FBI, I have investigated federal criminal violations related to high technology or cyber crime. I have gained experience through training and everyday work relating to conducting these types of investigations. Prior to becoming a Special Agent of the FBI, I earned a Bachelor's degree in Computer Science and Master's degree in Information Assurance, and was employed in the field of information security full time for thirteen years. Moreover, I am a federal law enforcement officer who is engaged in enforcing criminal laws, including 18 U.S.C. § 875, and I am authorized by the Attorney General to request a search warrant.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. § 875 (Interstate Communications) exists in THE PRODUCED INFORMATION. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

PROBABLE CAUSE

Background & Terms

Criminality of Threats in Interstate Communications

5. As defined in 18 U.S.C § 875, “Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both.”

Doxxing

6. Due to my training and experience, I know that “dox,” “doxed,” or “doxxing” refer to the practice of gathering personal or private information about an individual or a business and then releasing that information in a public forum, including the online internet release of such information, oftentimes with the intent to induce physical or mental harm to the individual.

Summary of Investigation to Date

7. On or about October 1, 2019, I was provided with information from an online tip submitted to the FBI National Threat Operations Center (NTOC) regarding threatening online communications against victim CD (abbreviated to protect victim identity) who resides in Australia. CD's complaint to NTOC contained details of online harassment and threats to CD and CD's seven year old daughter perpetrated by Kenneth Brant (Brant) located in Albuquerque, New Mexico. This complaint alleged that Brant had repeatedly harassed and threatened CD, including threats to rape and murder CD and her daughter. The complaint further alleges that Brant had doxed CD and her daughter. The complaint alleges that Brant had claimed to obtain a passport in furtherance of a plan to travel to Australia and carry out his threats. The complaint alleges that this threatening and harassing pattern of behavior was ongoing as recent as the date of the complaint's submission, August 10, 2019.

8. On or about October 3, 2019, I made contact with CD. CD confirmed the details of her online report, and additionally provided, by email, a set of documents purported to contain screenshots of email exchanges and forum posts related to these activities. CD also confirmed that the threatening and harassing pattern of behavior was ongoing to that date.

Violation of 18 U.S.C. § 875(c) by Brant

9. On or about October 4, 2019, I conducted searches in FBI databases for records of foreign travel by Kenneth Brant and for records of travel to the United States by CD. I was unable to locate any such records for the time period described by CD, and thus believe that all communications between CD and Brant were international in nature.

10. Included in the documentation provided by CD were communications sent from the email address kenbrant7@gmail.com to CD's personal email address in which the user of

kenbrant7@gmail.com wrote on or about October 7, 2018, "I've known about your daughter [CD's daughter]....I wanted to take a knife to [CD's daughter]'s jugular....and rape her in front of you...and if you decided to get me off of her...I'd stick the knife into her neck...that's all I wanted to do from the very very beginning."

11. Also included in the documentation provided by CD were screenshots of emails sent from the email address kenbrant7@gmail.com in which the user of kenbrant7@gmail.com wrote on or about September 25, 2018 "[...] And I'm going to 'dox' you, ok? [...] like post the information I said I would post on ICOM [...]" I know from the interview with CD that ICOM is an abbreviation for the internet message forum "Ice Cream on Mars."

12. Included in the documentation provided by CD were screenshots of public posts on ICOM in which the user "Reilly the 2nd" disclosed CD's full name, her date of birth, the town in which she lives, the name and age of her daughter, pictures of CD and CD's father, her email address, and her phone number. On the same forum, "Reilly the 2nd" also disclosed his own name as "Kenneth Donald Brant," his own birthdate as May 15th, 1991, and his own home address as 2306 Garfield Avenue SE Apt. 11, Albuquerque, NM 87106.

13. "Reilly the 2nd" also posted on ICOM, writing "Guys... I told my Australian internet girlfriend that I would rape her daughter..."

14. I believe that "Reilly the 2nd" and kenbrant7@gmail.com are both online accounts used by Brant for the following reasons:

- a. "Reilly the 2nd" posted that his own name was "Kenneth Donald Brant."
- b. Similarities between the email moniker kenbrant7@gmail.com and the name "Kenneth Donald Brant."

- c. “Reilly the 2nd” referred to threats to rape the daughter of an Australian national, and kenbrant7@gmail.com made threats to rape the daughter of CD, an Australian national.
- d. kenbrant7@gmail.com threatened to dox CD, a threat which the user of “Reilly the 2nd” then carried out.

15. I therefore believe that Kenneth Donald Brant did violate 18 U.S.C. § 875(c) when he made threats over the internet, in interstate or foreign communication, to rape the daughter of CD, an Australian national.

16. On October 21, 2019, a search warrant was authorized by the Honorable U.S. Magistrate Judge Kirtan Khalsa and later filed as 19-MR-1271 for the premises 2306 Garfield Avenue SE #11, Albuquerque, New Mexico 87106, Brant’s residence. On October 25, 2019, myself and other agents of the FBI executed this search warrant. Brant was present at his residence when the warrant was executed.

17. On October 25, 2019, the user of the ICOM account “28 yo virgin” created a public thread on ICOM titled “The FBI came to my apartment this morning.” In that thread, the user of the subject account made several public posts, writing “Posting for Australian woman. May need to get her ‘invovled’ [sic] now...the day I sent the email in question was October 7, 2018...And at that point I had concluded that she was trying to block me out of her life...All due to her fear of her life with her only daughter being tampered with...I KNEW that she DEATHLY feared anyone tampering with her life with her only daughter. She had told me about that.” Additionally, this thread contained what appears to me to be a copy of the text from the email sent by kenbrant7@gmail.com on October 7, 2018, which was earlier referenced in this affidavit.

The user of the subject account posted a photo with the caption “And here is my beautiful face” appearing to be of Brant.

19. Based on the information contained in the public posts made by the user of the “28 yo virgin” and “Reilly the 2nd”, it is reasonable to believe that the user of the accounts and Brant are one and the same and, further, that these accounts contain evidence of the transmission of interstate communications containing threats to injure the person of another, in violation of 18 U.S.C. § 875.

20. On November 1, 2019, the Honorable U.S. Magistrate Judge John F. Robbenhaar authorized a search warrant in the District of New Mexico, later filed as 19-MR-1344, for information related to “28 yo virgin” and “Reilly the 2nd.” This warrant was served on icecreamonmars.com the same day. On November 18, 2019, icecreamonmars.com produced information responsive to this warrant, THE PRODUCED INFORMATION. Agents began to analyze this data, but surmised that THE PRODUCED INFORMATION contained not just records of information related to the “28 yo virgin” and “Reilly the 2nd”, but records of information related to all accounts on icecreamonmars.com.

21. THE PRODUCED INFORMATION also contains supplemental information not sought by 19-MR-1344, which the government was not entitled to receive. However, because THE PRODUCED INFORMATION contains records related to all icecreamonmars.com activity, it is reasonable to believe that it contains the information sought by 19-MR-1344. Therefore, I request the issuance of a search warrant to search THE PRODUCED INFORMATION, more particularly described in Attachment A, and seize the items set forth in Attachment B.

BACKGROUND CONCERNING ONLINE FORUMS

22. ICOM owns and operates a free-access social-networking website of the same name that can be accessed at <http://www.icecreamonmars.com>. ICOM allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Online forums, like ICOM, allow users to create message “threads,” a container of public posts relating to a single subject, in which other forum users can participate in a public discussion by adding posts to the thread containing text, images, links, or other digital content. ICOM also provides a private messaging service that allows users of individual ICOM accounts to exchange messages that are not viewable by any but the sender and recipient accounts.

23. ICOM asks users to provide an e-mail address in order to create an account and associates that email address information with account activity. For each user, ICOM may retain information about the date and time at which the account was created, records of log-in times and durations, the types of service utilized, the methods used to connect to the account, and the Internet Protocol (“IP”) address at the time of sign-up. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a given forum account.

24. ICOM may retain records of user created content posted publicly or sent privately via servers controlled by ICOM. ICOM also keeps activity logs for each user. These logs contain information about the user’s activity including the date, time, and IP address associated with account access, thread creation, public posts, private messages, account modifications, and account log-offs. Additionally, ICOM may retain digital records of content posted by users to ICOM’s website that was later deleted or altered by users.

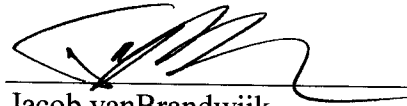
25. As explained herein, information stored in connection with an online forum account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a forum account’s user information, IP log, stored electronic communications, and other data retained by the forum owner, can indicate who has used or controlled the forum account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, communications, public posts, status updates, and posted photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the forum account at a relevant time. Further, forum account activity can show how and when the account was accessed or used. For example, as described herein, providers on online services typically log the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of forum access, use, and events relating to the crime under investigation. Last, forum account activity may provide relevant insight into the account owner’s state of mind as it relates to the offense under investigation. For example, information on the forum account may indicate the owner’s motive and intent to commit a crime (e.g., information indicating a criminal plan) or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

27. Therefore, the computers or servers in the control of the owners of ICOM are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of the ICOM forum, such as account access information, transaction information, and other account information.

CONCLUSION

28. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant applies to data already within the possession of the FBI, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Jacob vanBrandwijk
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on December 4, 2019



Honorable Kirtan Khalsa
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

This warrant applies to records and information (hereafter, THE PRODUCED INFORMATION) produced by icecreamonmars.com in response to a search warrant issued in the District of New Mexico and filed as 19-MR-1344, which is currently in the possession of the FBI, and is located at 4200 Luecking Park Avenue, Albuquerque, NM 87107.

ATTACHMENT B

INFORMATION TO BE SEIZED BY THE GOVERNMENT

All information contained in THE PRODUCED INFORMATION that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. § 875 (Interstate Communications) those violations involving those yet unnamed, including, for the accounts “28 yo virgin” and “Reilly the 2nd” hereafter THE SUBJECT ACCOUNTS, information pertaining to the following matters:

- (a) The contents of the electronic communications, subject to the limitations of the above paragraph, for the THE SUBJECT ACCOUNTS, including stored or preserved copies of posts, chats, or messages, sent to and from the accounts, draft messages, the source and destination addresses associated with each message or post, the date and time at which each post, chat, or message was sent, and the size and length of each post, chat, or message
 - 1. Tending to demonstrate the actual user(s) of the account;
 - 2. Relating to online threats or to other violations of 18 U.S.C. § 875.
 - 3. Account information for THE SUBJECT ACCOUNTS including:
 - (a) Names and associated e-mail addresses;
 - (b) Physical address and location information;
 - (c) Records of session times and durations;
 - (d) Length of service (including start date) and types of service utilized;
 - (e) Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address;

- (f) The means and source of payment for such service (including any credit card or bank account number); and
 - (g) Internet Protocol addresses used by the subscriber to register the account or otherwise initiate service;
 - (h) All filter and forwarding settings.
4. User connection logs for THE SUBJECT ACCOUNTS for any connections to or from THE SUBJECT ACCOUNTS. User connection logs should include the following:
- (a) Connection time and date;
 - (b) Disconnect time and date;
 - (c) Method of connection to system (e.g., SLIP, PPP, Shell);
 - (d) Data transfer volume (e.g., bytes);
 - (e) Internet Protocol addresses that were used when the user(s) connected to the service;
 - (f) Connection information for other systems to which user(s) connected via THE SUBJECT ACCOUNTS, including:
 - (1) Connection destination;
 - (2) Connection time and date;
 - (3) Disconnect time and date;
 - (4) Method of connection to system (e.g., telnet, ftp, http);
 - (5) Data transfer volume (e.g., bytes);
 - (6) Any other relevant routing information.

(g) Source or destination of any electronic communications sent from or received by THE SUBJECT ACCOUNTS, and the date, time, and length of the communications; and

(h) Any address to which electronic communications were or are to be forwarded from THE SUBJECT ACCOUNTS.

- (b) Evidence indicating how and when the accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;
- (c) Evidence indicating the account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used THE SUBJECT ACCOUNTS, including records that help reveal the whereabouts of such person(s).
- (e) The identity of the person(s) who communicated with THE SUBJECT ACCOUNTS about matters relating to violations of 18 U.S.C. § 875 (Interstate Communications), including records that help reveal their whereabouts.